SOPHOS

サイバーセキュリティ机上演習の実施方法

サイバー攻撃に備える机上演習のベストプラクティス

ソフォス ホワイトペーパー 2024 年 7 月

はじめに

机上演習では、攻撃を受けた状況をシミュレートし、計画している対策を実際に行うことにより、チームや対策のプロセスがどの程度適切に機能するかをテストします。机上演習は敵対的なシナリオに備えるための貴重な手法です。軍隊では、紛争状況におけるさまざまな戦略を試すために、また、政府は危機対応を改善するために機能演習を利用しています。企業にとって、机上演習はサイバー攻撃に備える効果的な手法です。

このガイドでは、サイバーセキュリティ攻撃に対する机上演習とは何か、そして、机上演習を実施する方法について説明します。このガイドで説明する方法は、ソフォスのサイバーセキュリティチームが攻撃に備えるために実際に取り入れているアプローチに基づいています。

ソフォスは長年にわたって透明性の確保を理念の一つとして掲げています。今回、ソフォスの戦略とリソースを共有できることを嬉しく思います。詳細な情報と資料については、トラストセンターを参照してください。

セキュリティ机上演習とは何か？

机上演習では、サイバー攻撃を受けた場合の対応と攻撃によって受ける可能性がある損害を確認できます。攻撃に対して自社がどの程度適切に対応できるのか確認することができ、サイバーセキュリティに関する洞察を得て、対応策を向上できます。

机上演習が重要である理由

盲点の特定：セキュリティの机上演習では、サイバーセキュリティの盲点を特定するために役立ちます。これにより、サイバー犯罪者によるこれらの盲点の悪用を防ぐことが可能になります。

セキュリティポスチャの分析：サイバーセキュリティの卓上演習では、自社のセキュリティポスチャを評価して最適化する方法を見つけることができます。

コミュニケーションの分析：サイバーセキュリティの机上演習では、サイバー攻撃に対応するときの障害となる可能性があるチーム間や部署間のコミュニケーションの問題を特定できます。

コンプライアンス：サイバーセキュリティ攻撃の机上演習を実施して文書化することは、厳格な規制が課せられている多くの業界のセキュリティプログラムにおいて、インシデント対応の要件となっています。

正確で迅速な対応：演習への参加者は、インシデントに対する模擬演習の対応を通じて、実際の攻撃で必要となる行動を正確かつ迅速に行うための能力を身につけることができ、対応を迅速化できます。

セキュリティ机上演習のタイプ

演習にはいくつかのタイプがあります。タイプによって必要な時間や効果も異なります。

即応シナリオ

ISACA は、即応シナリオについて「極めてハイレベルなシナリオであり、分かりやすく迅速に理解および議論することを目的としている」と定義しています。準備はほとんど必要なく、10 分～ 30 分程度で終了します。

即応シナリオには、さまざまな経歴を持つ初級、中級、上級のチームメンバーが参加できます。これらのチームメンバーには、十分な時間が与えられ、複数のシナリオを検討することができます。また、各チームメンバーがインシデント対応の担当者としてのそれぞれの役割を果たすことができます。

技術的対策の専用シナリオ

技術的対策の専用シナリオは通常、1 ～ 2 時間実行します。このようなシナリオでは技術的な深い議論が求められ、大規模な計画が必要となります。このシナリオでは、チームメンバーはセキュリティインシデントの技術的側面を評価できます。

技術的対策の専用シナリオでは通常、「シード」イベント（脅威の発生イベント）を用います。このイベントが展開されるときに、さらに詳細を追加することができます。このシナリオは、チームメンバーが複雑なサイバー攻撃に備えるために役立ちます。

すべての関係者が参加するシナリオ

すべての関係者が参加するシナリオは、技術的対策の専用シナリオを拡張したものです。このシナリオでは、技術的な問題と技術的以外の問題、そしてロジスティクスに重点を置いています。

すべての関係者が参加するシナリオは通常、2 ～ 4 時間がかかります。このシナリオに参加するチームには、技術的なチームメンバーに加え、法務、マーケティング、人事の専門家が含まれることがあります。

すべての関係者が参加するシナリオは、チームや部門間のコミュニケーションを改善することを考えている組織に最適です。すべての関係者が参加する机上演習には、技術者と技術者以外の担当者の両方を参加させると有益です。これにより、多くのチームや部門の参加者が集まり、一致協力してセキュリティの問題に取り組む機会を得ることができます。

チームや部門がこのシナリオの異なるタイミングで参加するように求めている組織もあります。これにより、チームや部門は、実際のセキュリティインシデントが発生した場合と同じように対応に関わることができます。

セキュリティ机上演習を実施するのは誰か？

セキュリティ机上演習は、外部チームが実施することも、社内チームが実施することもあります。

外部チームによる実施

セキュリティ机上演習を提供しているサードパーティのサービスプロバイダーは、シナリオの進行を管理し、組織にディスカッションを促します。外部チームがシナリオを実施する場合、シナリオの設定や運用に関する労力はほぼ不要です。

外部プロバイダーは通常、組織や環境に合わせた机上演習を実施します。通常、外部プロバイダーは対象となる企業のビジネスとセキュリティ上の課題を理解してから、その企業の状況に合わせてカスタマイズしたセキュリティ机上演習を開発します。

社内チームによる実施

自社独自のセキュリティ演習を開発することができます。机上演習を社内で開発して実施するにはコストと時間がかかりますが、サイバーセキュリティ演習を自社の特性や環境に合わせて詳細にカスタマイズすることができます。例えば、このような机上演習では、参加者が日常的に使用しているシステムを使用することで、現実により即したシナリオとなり、参加者にとって机上演習の意義がより深くなる場合があります。

また、社内チームが実施する机上演習では、参加者が協力して、組織、従業員、顧客に直接影響を与える具体的な問題を特定して対応できるようになります。

ソフォスのアプローチ

ソフォスでは、特定のチームや部門向けに、サイバーセキュリティの机上演習をカスタマイズして実施しています。ある机上演習では通常、セキュリティに関する軽微な問題から始め、参加者同士でどのように対応するかなど、アイデアを出し合うように促します。さらに、「特定された情報」から、問題の重大性を判断します。

以下に、ソフォスが実施しているサイバーセキュリティの机上演習のシナリオのテーマの一部を紹介します。これは各企業が自社独自の机上演習を開発して実施するときに利用できます。

チーム	シナリオ
Sophos X-Ops	インサイダーの脅威
人事	ランサムウェアと従業員の個人情報の漏洩
テクニカルサポート	顧客を装った標的型攻撃
マーケティング	従業員のセキュリティが侵害され、会社の Web サイトやソーシャルメディアが改ざんされた。
法務	悪意のあるバグ報奨金の研究者
Sophos X-Ops	侵害されたアナリストのシステム、サプライチェーン攻撃
エンジニアリング	侵害されたソフォスのバイナリ、サプライチェーン攻撃
エンジニアリング	フィッシング攻撃を受けたエンジニア
IT	大規模なランサムウェアインシデント
エンジニアリング	アプリケーションのゼロデイ脆弱性によって、顧客ベースが侵害された

セキュリティ机上演習を開発するときのベストプラクティス

以下に紹介するベストプラクティスは、効果的なセキュリティ机上習を自社で開発するときに役立ちます。

1. 机上演習に参加する対象者を特定する

対象者を決定してから、サイバーセキュリティのシナリオを作成します。例えば、サイバーセキュリティチームをテストする場合は、セキュリティに関する複雑な対応が求められるシナリオが理想的です。一方で、IT チームや DevOps チームをテストする場合は、参加者がシナリオを理解し、時間と労力、そして注意を払う価値のある問題を選択します。

2. 適切な参加者を選定する

セキュリティ机上演習のシナリオに参加してもらう対象を、単一のチームまたは部署にするのか、複数のチームや部署にするのかを決定します。単一のチームが参加するシナリオでは、参加者がサイバー攻撃にどのように対応するかを確認できます。一方で、複数のチームや部門が参加する場合、異なる事業部門の関係者が協力してセキュリティインシデントに対応できるようになります。

3. 参加者がシナリオに加わるタイミングを見極める

さまざまなチームや部門がサイバーセキュリティのシナリオに参加するタイミングを検討します。例えば、組織が保存している個人情報（PII）が漏洩した場合、GDPR やその他のデータセキュリティ要件を確実に遵守するために、法務チームのメンバーに参加してもらう必要がある場合があります。

セキュリティ机上演習のシナリオでは、組織のすべてのチームや部署から少なくとも 1 人を参加させると有益となることが多くあります。このようにすることで、インシデントが発生したときの部門間のコミュニケーションとコラボレーションが円滑になります。

4. 参加者の人数を決定する

シナリオを実施するときには、必ず参加者同士が関わり合い、共通の目標を達成するために協力するようにしてください。ソフォスが取り入れているシナリオでは、チームや部門のいくつかの役職、あるいは複数のチームや部門に所属しているメンバーが参加し、多くの場合、最大で 25 人が参加します。セキュリティ机上演習に参加する人数を決定するときには、組織の規模、チームや部署の構成を考慮してください。

5. 演習時間を管理する

机上演習を完了するための十分な時間を参加者に与えてください。ソフォスは、長時間の机上演習のセッションは避けるようにしています。数時間以上に及ぶセッションになると、参加者がスケジュールを調整し、参加するのは困難になります。

6. 資料を準備する

PowerPoint のプレゼンテーションなどの資料を使用してシナリオを伝えてください。ソフォスのチームは通常、机上演習用の PowerPoint のプレゼンテーションを使用し、各スライドにはイベントの進行と参加者に検討してもらう質問を記載しています。ソフォスでは通常、このような机上演習用の PowerPoint プレゼンテーションを 20 枚のスライドに制限しています。

7. 机上演習のストーリーを作成する

実際の攻撃を想定したストーリーを作成し、そのストーリーに沿って取り入れる情報を調整します。最近ニュースになった攻撃などを取り入れると、参加者の関心を高めることができます。大規模なストーリーを作成する場合、ストーリーに関連するシステムやログに重要な情報である印を付けて、参加者が簡単に見つけて利用できるようにします。

8. 参加者に合わせた机上演習を作成する

参加者のセキュリティの成熟度 (知識や経験レベル) に基づいて、サイバーセキュリティの机上演習を作成してください。例えば、参加者のサイバーセキュリティのスキルや専門知識が豊富な場合には、詳細なストーリーを作成すると有益です。参加者のスキルや専門知識があまりない場合には、一般的で概要レベルのシナリオが最適となるでしょう。

詳細なシナリオを作成する場合は、現実的な攻撃シナリオを反映していることを確認してください。例えば、組織やネットワークの特定の部分を対象とした机上演習を行う場合には、その分野について詳しい知識のある方から情報を収集して知見を得るようにしてください。こうすることで、参加者が共感できるシナリオを作り上げることができます。

9. 参加者のフィードバックを取り入れる

参加者に、机上演習に取り入れることができるアイデアがないか聞いてみましょう。参加者の多くは、日々の業務で遭遇しているセキュリティのペインポイントに関する知見を持っており、共有することができます。これらのペインポイントを取り入れたシナリオを作成すると、参加者が将来的にこれらの課題を解決する方法を見つける上で役立つ場合があります。

10. シナリオを詳細に計画する

シミュレーションした攻撃を展開する方法をフロー図に落とし込みます。こうすることで、机上演習のストーリーで欠けている要素を特定するのに役立ちます。また、ストーリーで解決した問題について理解しているチームや部門のメンバーにもフィードバックしてもらいます。これらのチームや部門のメンバーは、問題を解決し、シナリオが現実に沿っていることを確認するのに役立ちます。

11. 議論する質問を作成する

ストーリーを作成するときに湧いてくる質問や疑問を書き留めておきましょう。これらの質問は、シナリオの参加者同士の議論を促進するために利用できます。

12. ストーリーを確認する

参加者に伝える前に、シナリオを何度も見直して評価してください。参加者がストーリーを最後まで実行するのにかかる時間を判断することは難しい場合があります。机上演習で必要となる時間について不確定な部分がある場合は、慎重に検討を重ねて時間を正確に特定できるようにしてください。プレゼンテーションで説明しているシナリオの時間が、参加者が実施できる制限時間いっぱいになったり超えたりする場合は、必要に応じて修正してください。

13. 机上演習のトーンを設定する

参加者が机上演習を開始するときには、参加者の年齢や勤続年数に関係なく、全員が参加するよう奨励します。この机上演習は、すべての参加者が自分の意見を出し合い、組織のセキュリティポスチャを改善する大切な機会になります。参加者同士が積極的にコミュニケーションして、協力し合うほど、参加者全員がこの机上演習からより大きな価値を得ることが可能になります。

14. 机上演習の進行を管理する

進行の管理は、演習を時間どおり正しく進めるために重要です。ただし、進行管理者は演習には参加しないようにしてください。進行管理の担当者は、参加者にシナリオを提供して、参加者がシナリオを進めるための支援に専念してください。また、ストーリーのさまざまなトピックについて参加者が話し合う時間を設けたり、議論する質問や重要な情報を共有したりすることもできます。

15. 問題を追跡する

机上演習を実施するときに発生した問題について、誰かがメモを取っていることを確認してください。ストーリーの効果を妨げる可能性のある問題について有用な情報を得ることができます。

16. 机上演習の時間を管理する

演習のタイマーをセットし、時間を厳格に管理してください。参加者が正しく演習を進め、ストーリーの進行に合わせて作業を続けることができるようにしてください。

17. 結果を確認する

机上演習を実施した後は、演習の結果と、組織の日常業務にその結果をどのように取り入れることができるかを検討します。例えば、コンプライアンス要件に基づいてテストを完了した場合、監査人が必要とする情報が含まれる PDF を作成できます。

また、参加者が机上演習で得られた所見を確認する機会を設けて、同じ演習を後日行うこともできます。同じ演習を繰り返すことで、最初の演習で特定された問題への対応を修正または変更し、問題を解決できるようになったかどうかを確認することができます。

ランサムウェア机上演習の例

ソフォスで作成および実施しているランサムウェア攻撃の机上演習のストーリーを以下に紹介します。ランサムウェア机上演習。

このストーリーを直接使用することも、カスタマイズして独自のストーリーを展開することもできます。

サイバーセキュリティの机上演習の資料

米国サイバーセキュリティ・社会基盤安全保障庁 (CISA) は、企業が独自の机上演習を実施するときに役立つ資料を提供しています。以下のシナリオを含むさまざまな脅威に対応するように設計されている 100 以上の CISA 机上演習 (CTEP) を利用できます。

- ✓ サイバーセキュリティ : ランサムウェア、インサイダーの脅威、フィッシング、産業制御システム (ICS) の侵害、その他のサイバーセキュリティに関連するシナリオが含まれます。
- ✓ 物理的セキュリティ：銃乱射、車両突入、即席爆発装置 (IED)、無人航空機システム (UAS)、その他の物理的セキュリティに関連するシナリオが含まれます。
- ✓ サイバー攻撃による物理的な影響と物理的な攻撃によるサイバー環境への影響：サイバー攻撃の脅威による物理的な影響と、物理的な攻撃によるサイバー環境への影響を中心したシナリオが含まれます。

これらのシナリオに加えて、CISA は構築済みのテンプレートを提供しています。これらのテンプレートを使用して自社独自の机上演習を開発できます。

まとめ

机上演習が有効であることが実証されており、現在のサイバーセキュリティ対策において重要な役割を担っています。今のデジタル時代ではサイバー攻撃の脅威が蔓延しています。組織は業務を保護するためにこれらの机上演習を取り入れて実施しなければなりません。セキュリティ机上演習の基本要素を理解し、本書で概説したベストプラクティスを実施することで、サイバー攻撃に対するレジリエンスを強化し、サイバー攻撃に直面したときにその影響を軽減するための準備を整えることが可能になります。

ソフォストラストセンター - https://www.sophos.com/ja-jp/trust

ソフォスのランサムウェア机上演習 - https://assets.sophos.com/X24WTUEQ/at/hvsj54g5zq5hhcfb3xrfnmk/sophos-ransomware-tabletop-exercise-overview.pdf

CISA 机上演習 -https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

ソフォスは透明性の確保を理念の一つとして掲げています。
詳細な情報と資料については、トラストセンター
(www.sophos.com/trust) を参照してください。

2024-07-24 (WP-DD)

SOPHOS